A Secure Loading Routing Protocol in IOT using Block Chain Technology

Suresh Mundru [1], K Meena [2]

[1] *CSE Department*, KKR&KSR Institute of Technology & Sciences, Andhra Pradesh, India.
[1, 2] *CSE Department*, Vel Tech Rangarajan, Dr. Sagunthala R&D Institute of Science and Technology,Chennai-600062, India.

***Abstract* - Internet of Things (IoT) plays a more imperative part with its performance, its uses range from usual hardware to broad family uses such as WSNs and RFID. With the considerable capability of IoT, there comes a wide range of difficulties. This paper focuses on different routing protocols and the security problems among them and other challenges. We focus on secure LOADING routing protocol with block chain technology. Block chain technology plays a major role for providing integrity and authentication. The protocol is evaluated with NS2 and the performance of LOADING protocol is compared with LOAD protocol and AODV protocol.**

Keywords - Iot, Block Chain, Loading, Aodv, B-Loading.

I. INTRODUCTION

Internet of Things (IoT), also called as machine-to-machine is a new communication model, which offers both chances and challenges. Always, humans keep demanding technologies to save money and time. Basically, human beings want to be happier, human beings becomes more happier when they have following things, First, humans want further time and money to lead the life joyfully and improve the quality of life. Use of Technologies helps in saving money, enhancing their appearance and eating better. Second, most of all the human beings want to escape being in nasty situations. Technologies like estimation of environmental changes or fire warning systems helps in predicting the future events. Third, human beings hunger to be healthier. Earlier it was very difficult to identify the information flowing in network but now more network altering capabilities are budding. First, different natures of sensors improve our perceptual skills by sensing information that humans not able to sense and gather such information anytime and anywhere. Second, robots advance our skill to perform better where humans cannot reach by overcoming physical limitations during natural disasters. Robots can perform better-than-human skills, for example robots were used to explore the destruction caused by the nuclear plants due to radiation in Japan [2]. Third, wireless communication and broadband technologies increase our quality of communication facilities only when 4G wireless [3] and improved internet bandwidth become available. Fourth, growing cloud computing and machine intelligence technologies will improve quality of analytical skills by gigantic computations and advanced machine learning practices. Technologies provide information on human's well-being and environmental hazards, to take care of geriatric and unhealthy people, and to escape accidents and injuries. Fourth, most people wish for friendship, using E-mail, smart phones and social networks like Face book, Twitters and Whatapp and etc., which connect people. Ultimately, people need to be extraordinary and to be appreciated [1]. The emerging M2M technologies fulfil the above listed human wishes [4] [5] [6]. For example, imagine that you are going to give a talk in continued medical education program in another metropolitan city and you got stuck in traffic. Improvement in communication technology enables your calendar and your car can link together and your smart phone automatically sends message to your meeting regarding delay in arrival. The challenges now a days we are facing from IOT mainly was routing and security.

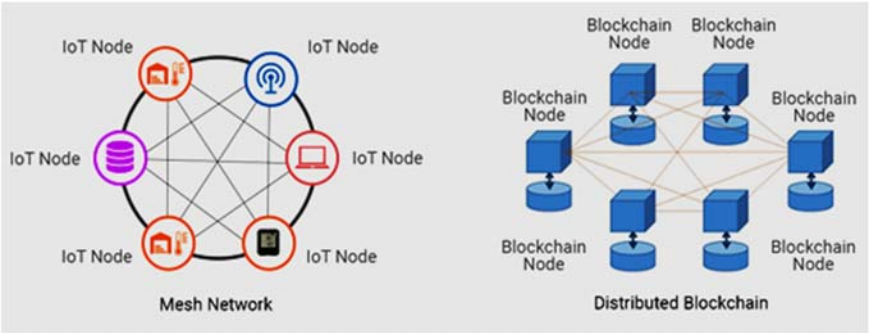

Figure 1. IOT and block chain IOT

Presently, we have number of routing protocols for IOT. But no one gives the secure communication for that we are using most adaptive and strong secure mechanism called block chain and we use this block chain based LOADING protocol in routing which gives more secure and reliable communication in IOT devices. We performed simulations using NS2. The rest of the paper was organized as follows Section 2 gives a comprehensive view of state of the art. Section 3 provides proposed work, next section provides Results and experiments.

II. STATE-OF-ART

In averting routing assaults, a few secure routing techniques have been proposed In this area, we exhibit a review of the diverse secure routing conventions. Secure multi-jump routing for IoT interchanges The Secured Multi-bounce Routing Protocol (SMRP) which enables IoT gadgets to convey in a safe way. It achieves this by ensuring that IoT gadgets authenticate before they could join or make another system. The routing protocol proposed consolidates a multi-layer parameter into the routing calculation and subsequently, when hubs need to join the network they need to validate. This convention accompanies no additional overhead on the routing procedure as the multilayer parameters contain the reasonable applications on the network, a remarkable User-Controllable Identification and a synopsis of devices permitted on the network. A trust-based secure routing structure in wireless sensor networks: Trust-based secure Routing Framework (TSRF) planned for WSNs depended on trust inference which comprises of direct and roundabout perceptions of behavioural examples of sensor hubs with trust esteems among hubs spoke to in a range from 0 to 1 A 0 meaning no trust exists between hubs and demonstrating a decent level of trust for the comparing node. Two-way Acknowledgement based trust (2-ACKT) This framework works in a non-indiscriminate mode and is contingent just on coordinate trust between hubs. The scheme is in light of a double affirmation framework in developing trust among neighbouring hubs[9]. The plan facilitate develops a course to the sink hub and in addition presented another node(regarded as the support and outsider hub) which creates a two jump affirmation in the system. One essential assumption the convention makes is, that every malignant hub drop data packets and not the affirmations subsequently, it can't isolate grey hole attacks. The gathering based trust administration scheme[10] .The Group-based trust administration conspire (GTMS) which is a trust based plan including the calculation of trust via an immediate perception among hubs i.e. the number of successful and unsuccessful connections[12] among hubs .

III. BLOCK CHAIN TECHNOLOGY IN IOT

Block chain is initially utilized for recording money related exchanges, where exchanges are encoded and kept by all members. Subsequently, all exchanges are straightforward and any adjustments can be effortlessly followed and distinguished [11]. Square tie can be connected to upgrade security of IoT. We will now introduce two cases of utilizing Block chain for IoT security. At the point when datasets are shared among the exploration and specialist groups or all the more generally, their honesty ought to be kept up. In our specific situation, to guarantee uprightness of the datasets, a Reference Integrity Metric (RIM) for the dataset is kept up utilizing Block chain. In particular, at whatever point a dataset is downloaded, its respectability can be checked utilizing the RIM. No security strategy is worst proof, and IoT gadgets and frameworks could be traded off regardless of the best (security) endeavours. In this manner, we need the ability for traded off gadgets to self heal. We recommend utilizing block chain to encourage self-mending for bargained gadgets.

IV. PROPOSED WORK

AODV routing protocol is the basis for LOADing, which uses the reactive approach. In reactive approach, whenever data to be send then only it creates the routes towards destination. In LOADing whenever node wants to send data it checks the routing table for the possible route to the destination. To find feasible path LOADing floods the RREQ message in the network [13]. Once node receives the RREQ message, the node checks for the destination node by itself, If not it forwards the RREQ to neighbouring nodes. When destination node receives the RREQ message it responds to the request originator by unicasting the RREP message [8].

The main drawback of the LOADing is delay in the route discovery. During route discovery phase outgoing packets are buffered in the nodes, this may cause the packet loss in the resource constraint devices. The nodes are suffered from energy depletion because of flooding. Another drawback of this protocol is collision. Packet collisions are more due to the flooding, which leads to redundant retransmission of data [8]. And also the security aspects of the routing protocols.

A LOAD routing protocol based on AODV is proposed. The developed LOAD reduces the implementation complexity and provides load balancing in the network as compared to AODV [14]. It preserves the routing table and route request table that are used in route detection phase.

LOAD does not use the predecessor of AODV as Route Error message is sent to source only. Further the protocol does not use the target succession number that

results in lessening of packet size and simplify path identification process [15]. The reply for the Route Request (RREQ) message is sent only from the destination node which ensures loop free condition. Link Quality Indicator (LQI) of LOAD protocol MAC layer as a routing cost metric to determine the strongest route is used in the proposed method. It uses Acknowledge message to represent successful packet transfer.

A. Algorithm for LOADing:

LOAD uses RREQ packet for establishing route
LOAD broadcasts RREQ packet, whenever Receiver receives RREQ packet it simple broadcasts RREP packet back to the source.
It preserves routing table and route request table during path identification phase
LOAD uses the Link Quality Indicator (LQI) of LOAD MAC layer.
LOAD sends the data whenever route is established.

This traditional LOAD routing protocol suffer from privacy and authentication problem and malicious node activities. In order to secure routing using LOAD we use block chain technology. Here initially we configure special nodes which we can call them as miner nodes those nodes maintain the separate blocks for each activity. That is, whenever a node starts communication it starts recording the communication. It generally starts the recording the communication that is whether the node is forwarding the packets or dropping the packets [16].If a node uses to drop the packets so these will add those nodes to the blocked list. In next routing those nodes will not be added to the routing [17]. Like that the miner node stops the malicious activities and also these suggest the better routes for communication.

B. Algorithm for LOADing using Block Chain Technology

Step-1: Sender transmits a RREQ packet
Step-2: Miner node records the sender and receiver details
Step-3: whenever route is established it records all the communication of the intermediate nodes
Step-3.1: It has already previous knowledge or rules in the separate blocks
Step-3.2: if it violates more than the threshold, The node is added to the block list
Step-3.3: otherwise that route information is also added to the block data and the procedure is continued.
Step-4: whenever if a route is failed the nodes again regenerate the RREQ packet and transmit over the network.
Step-5: The procedure is continued

V. EXPERIMENTAL EVALUATION

We have done the experimental evolution of LOADING protocol with the most reliable simulator NS2. And we compare the secure routing of LOADING protocol with and without block chain technology. The experiments are done in UBUNTU operating system, NS-2.35. The simulation parameters as follows,

VI. RESULTS AND DISCUSSIONS

Throughput comparisons: Throughput is the amount of data packets successfully received with in the stipulated time is called as throughput.

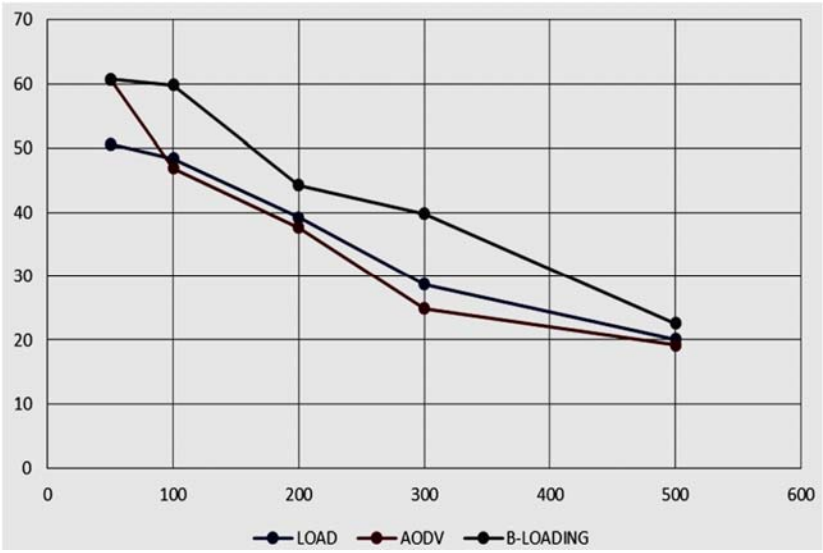

Figure 2. Throughput compressions of LOAD, AODV and Block chain

LOADING protocols the results shows that B-LOADING protocol gives more throughput because it almost cot each and every malicious nodes in the network so that it gives more throughput.

E2E Delay: E2E Delay is the time taken a packet to travel from the source to the target.

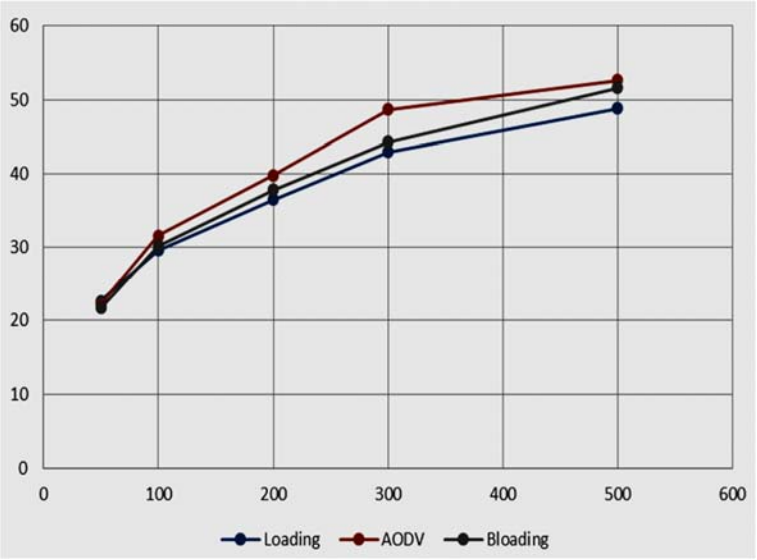

Figure 3. The E2E delay compressions of LOAD, AODV and Block chain LOADING protocols

The results shows that B-LOADING protocol have median E2E delay than two because it takes more time in computing the black chain propagation in the network so that it has medium E2E delay.

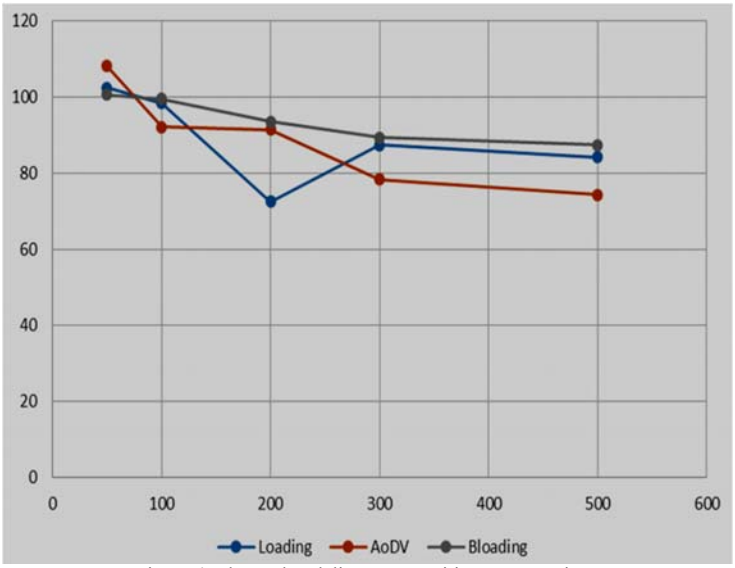

Figure 4. The packet delivery proposition compressions

PDR: the ratio of number of packets successfully transmitted from source target is called PDR. Figure-4 shows the packet delivery proposition compressions of LOAD, AODV and Block chain LOADING protocols the results shows that B-LOADING protocol gives more PDR because it almost cot each and every malicious nodes in the network so that it gives more PDR.

VII. CONCLUSION

This paper focuses on the different routing protocols and the security problems among all and other challenges. And also we are focusing on secure LOADING routing protocol with block chain technology. Block chain technology plays major role for providing integrity and

authentication. The protocol is evaluated with ns2 and the performance of LOADING protocol is compared with LOAD and AODV protocol. The performance result shows that LOADING performance is better in all aspects than other routing protocols.

REFERENCES

[1] J. DESJARDINS, It's official: Bitcoin was the top performing currency of2015, 2016.

[2] J. Adinolfi, And 2016's best-performing commodity is ... bitcoin? 2016.

[3] Block chain.info, Confirmed transactions per day, 2017. URL https://blockchain.info/charts/n-transactions?timespan=all/#.

[4] Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for block chain in healthcare: medrec prototype for electronic health records and medical research data, 2016.

[5] Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using block chain for medical data access and permission management, in: International Conference on Open and Big Data, OBD, 2016, pp. 25–30.

[6] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Health care data gateways: Found healthcare intelligence on block chain with novel privacy risk control, J. Med.Syst. (2016) 218.

[7] S. Huckle, R. Bhattacharya, M. White, N. Beloff, Internet of things, blockchainand shared economy applications, Proc. Comput. Sci. 98 (2016) 461–466.

[8] P. Bylica, Ł. Gleń, P. Janiuk, A. Skrzypczak, A. Zawłocki, A probabilistic nanopayment scheme for golem, 2015. URL http://golemproject.net/doc/GolemNanopayments.pdf.

[9] P. Hurich, The virtual is real: An argument for characterizing bitcoins as private property, in: Banking & Finance Law Review, Vol. 31, Carswell Publishing,2016, p. 573.

[10] Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Block chain for IoT security and privacy: The case study of a smart home, in: IEEE Percom Workshop onSecurity Privacy and Trust in the Internet of Thing, 2017.

[11] Y. Zhang, J. Wen, The IoT electric business model: Using block chain technology for the internet of things, Peer-to-Peer Netw. Appl. (2016) 1–12.

[12] J. Sun, J. Yan, K.Z. Zhang, Block chain-based sharing services: What block chain technology can contribute to smart cities, Financ. Innov.(2016) 26.

[13] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The block chain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 2016.

[14] E. Nordström, Personal Clouds: Concedo (Master's thesis), Lulea University of Technology, 2015.

[15] J.S. Czepluch, N.Z. Lollike, S.O. Malone, The use of block chain technology in different application domains, in: The IT University of Copenhagen, 2015,Copenhagen.

[16] Ethereum, Etherscan: The ethereum block explorer, 2017.

[17] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.

[18] V. Buterin, Critical update re: Dao vulnerability, 2016. https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

[19] J. Adelstein, Behind the biggest bit coin heist in history: Inside the implosion of mt.gox, 2016.

BIBLIOGRAPHY

Suresh Mundru is a research scholar of Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai. He received his B.Tech Degree in Computer Science and Engineering from JNTUH, Hyderabad in 2005 and received M.Tech Degree in Computer Networks and Information Security from JNTUH, Hederabad in 2011. He is currently Assistant Professor in Computer Science and Engineering, KKR&KSR Institute of Technology and Sciences, Guntur. His Research interests include Data Mining, Big Data, Internet of Things, Network Security and Cyber Security.

??

Dr K. Meena received a Ph.D in Computer Science from the Department of Computer Science and Engineering, Manonmaniam Sundaranar University, India in 2014. She received the degrees of B.E. (Electronics and Communication Engineering) and M.E. (Computer Science and Engineering) from the same University in 2002 and 2009. She is currently Associate Professor in Computer Science & Engineering Department, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai. Her research interests include Machine Learning, Pattern Recognition, Image Processing, Biometrics and Cyber security. She has published 30 international journal papers, 7 international conference papers and 11 national conference papers.